CAN A SELF-DIAGNOSTIC DIGITALLY CONTROLLED PACEMAKER/DEFRIBRILLATOR DEVICE BE USED FOR ALERTING MILITARY PERSONNEL WHEN A SOLDIER HEALTH CONDITION BECOMES COMPROMISED OUT IN THE FIELD

Steven Nedd
U.S. Army TARDEC
Warren, MI. 48397-5000

ABSTRACT

The Self-Diagnostic Digitally Controlled Pacemaker/Defibrillator Device (SDDCPDD) has several features that I think may be very useful to the Armed Services. Even though this device is designed as a pacemaker/defibrillator device; its applications can be used as a sensory data retrieval device for Soldiers that have been captured in the field or in combat missions.

This research investigates the use of Unified Modeling Language (UML) Diagrams, Object-Oriented Analysis and Design, and Structured Query Language (SQL) to develop the high level architecture of a system to store and retrieve digital/wireless communication information from a pacemaker/defibrillator, or other device to determine the whereabouts, and alert military personnel of the status of the Soldier. It presents the requirements and architectural design of the Self-Diagnostics Digitally Controlled Pacemaker/Defibrillator Device.

1. INTRODUCTION

Pacemakers and defibrillators have made quantum leaps in capabilities since its technology began over 200 years ago when such pioneers as Luigi Galvani and Alessandro Volta brought about the awareness of electricity, biology, and electro-chemistry. Volta, whose name is synonymous with the rating of batteries (Volts), did remarkable studies in the area of electricity and electrical current. Galvani's conclusions lead him to study the theory of neurophysiology, neurology, and the electrical nature of nerve-muscle function. In 1947 Dr. Claude Beck defibrillated the first human heart. Dr. John Hopps' concepts, innovation, and theory of the pacemaker came to acknowledgement in 1949. Kouwenoven and Milnor made other contributions with their 'closed chest capacitor-discharge defibrillator', and Zolls in 1954 with his success on the first external defibrillator on the human heart. Hopps led others to become interested in the pacemaker, and several years later (1957-1958) Earl E. Bakker made a breakthrough with the design of the first wearable pacemaker. It was not until the advancement of transistor technology that pacemakers became smaller. Transistor technology enabled processors to become an integral part of the pacemaker design, which later allowed the device to become even smaller, software embedded, and implantable. In 1984, pacemaker technology had advanced to the point where a pacemaker was small enough to be implanted into the chest cavity of a human. The first case of this experiment was done on a premature baby born in Calgary. This became the benchmark for pacemakers, and the very first operation of its kind in the world. [i]

Current pacemakers are very small (See Figure 1); about the size of two silver dollars stacked on top of each other (or two-inches wide and a quarter inch thick), and very easily implanted in a small pocket above the cavity of the chest. The pacemaker also has programmed pacing functions, histogram functions, and shock sensing control algorithms to control the amount of shock needed by the individual. It also has a reprogramming function within the device that allows reprogramming of the device over the telephone instead of going to the doctor. This is where the Military Device or Self-Diagnostics Digital Controlled Pacemaker/Defibrillator Device (SDCPDD) comes into play. It will be used to alert military personnel when a Soldier's health condition becomes compromised and assistance is needed in the field. The Military Device would be mounted on the body in places where vitals can be gathered, yet shielded from sight.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
26 SEP 2006	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Can A Self-Diagnostic Digitally Controlled Pacemaker/Defibrillator Device be Used For Alerting Military Personnel When a Soldier Health Condition Becomes Compromised Out in the Field?	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) **Nedd, Steven**	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **USATACOM 6501 E 11 Mile Road Warren, MI 48397-5000**	8. PERFORMING ORGANIZATION REPORT NUMBER **16429**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S) **TACOM TARDEC**
	11. SPONSOR/MONITOR'S REPORT NUMBER(S) **16429**

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**SAR**	**8**	

Figure 1. **Today's Pacemaker**

2. AREAS OF RESEARCH

This research explores the concept of allowing a pacemaker/defibrillator/ military device to become self-diagnostic, individual specific, and serialized, therefore, allowing stored information within the device to be sent via wireless communication to a database, data warehouse/data store, medical, and/or command and control for future reference, statistics, and history.

Research Questions

- Can software be used to send and update real time data to and from a data warehouse/data store?
- Can this device be used as a security device to alert medical or command and control when the device has gotten into the wrong hands?
- Can this information be sent via digital signal/control and wireless communication to a database without signal interruption?
- Is safety a concern and will this device cause harm?

3. SCOPE

The goal of this paper is to create awareness and possibly demonstrate the strength and viability of having a self-diagnostics scheme with digital control and wireless communication to be embedded in a military device.

4. METHODOLOGY

Already available Off-The- Shelf Software (OTS) and Commercial-Off-The-Shelf (COTS) items can be used to design a device that has multi-functional uses given the right application and environment.

5. OBJECTIVE

The military device, very much like the pacemaker/defibrillator, will be used to determine the medical condition (heart rate, pulse, breathing condition, and other vitals) of the person wearing the device. In addition, the device will record this information, and have it ready to be sent every 8 hours to a storage device (data warehouse/data store), medical, or command and control. The system can also send a digital signal activating an alarm when an individual's health condition is compromised. The medical examiner can then analyze the sent data, determine whether or not this condition is a condition of concern, and take the appropriate action to get help to that individual.

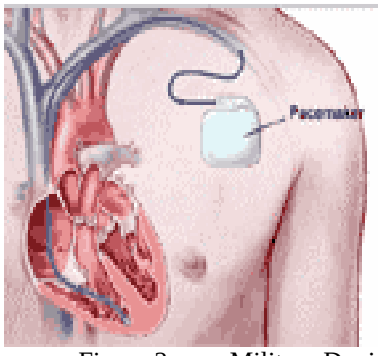

Figure 2. Military Device

6. DATA WAREHOUSE/DATA STORE/SECURITY

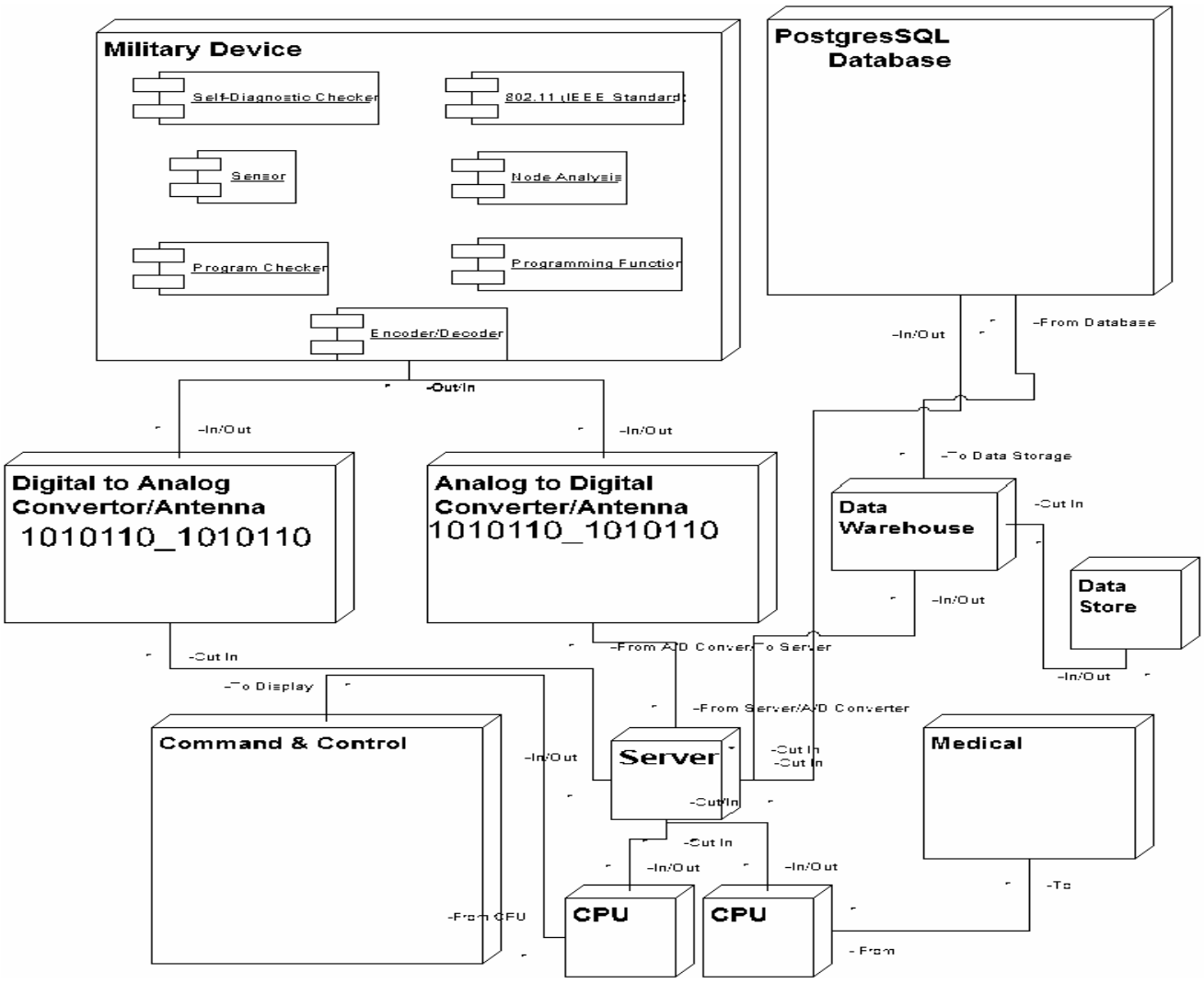

Figure 3. Military Device Deployment Diagram Digital Communication

The data store is also subject-oriented, integrated, and provides a detailed-only collection of data that will provide the component of the decision support system that acts as a database for storage of the data that is used in the Military Device. The data for the Military Device will be used for keeping track of operational events, driven history and data exchange.

SQL on the other hand is used to communicate often with databases. It is also used is to update, retrieve, and store data into a database. Data security is mandatory for military applications. SQL has the capacity to address important issues such as data security and data integrity. Data security handles the issues of confidentiality and authorized data access. SQL can provide interaction with other databases by using common commands such as the '"Select", "Insert", "Update", "Delete", "Create", and "Drop" commands. These commands provide the capability to accomplish all tasks needed to update, retrieve, and store historical data into a database.

According to the American National Standards Institute (ANSI), SQL is the standard language for relational database management systems (RDMS). SQL has the capability of enhancing digital communication interactions for sending and receiving signals (see Figure 3). The intended database must be capable of storing, retrieving, updating, uplinking, downloading, and securing sensitive information about a particular individual. The sensitive nature of the device and design requires a data warehouse that can accommodate these features with security and data integrity. The application of choice for the SDDCPDD was PostgresSQL; however, because of the nature of security the military may consider using another method of routing and storing information.

The SDDCPDD would require an antenna or device that would allow the signals to be sent by free space, and power magnification. Power magnification has a lot to do with the doubling of the range in which you want to send your signal. The 2.4 GHz ISM Frequency Band is becoming the world-wide standard in sending digital signals over the airways, via wireless internet, and cell phones. An antenna would have to be investigated to achieve the range needed to send or retrieve digital/wireless information to the database/data warehouse. The 802.11 (IEEE standard) Wireless Network Device or the like is ideal for accomplishing the task of sending signals in free space from the Military Device or SDCPDD, to the ORDBMS, data warehouse, and all routes back and forth and in between. A very weak signal could and would have to be boosted, and then amplified to allow a weak signal to be transmitted to the transmission station to carry the information back and forth to its destination. Algorithm and frequency hopping is critical for achieving signal amplification. Voltage gain is another factor in achieving signal strength and transmission power. If $A_{v\ SDDCPDD}$ is the voltage gain coming out of the self-diagnostic digitally controlled pacemaker/defibrillator device and the station voltage gain is called $A_{v\ station}$, then if $A_{v\ SDDCPDD}$ = 10 dB and

$A_{v\ station}$ = 100 dB, then the total voltage gain of the SDDCPDD and the station = 10 x 100 = 1000. The decibel equivalent of voltage gain ($A_{v\ total}$) => 1000 = 20 log 1000 = 20 x 3 = 60 (dB). This is the gain needed to get the signal to its destination. Frequency hopping is used by many wireless networking devices and applications, and the 802.11 (IEEE standard) seems to be the best device for the SDDCPDD.

The 802.11 (IEEE standard) Wireless Networking device seems to be a better choice over Bluetooth, and HomeRF.

The table below provides a comparison between the three.

802.11 (IEEE Standard)	Bluetooth	HomeRF
2.4 Ghz (ISM band)	2.4 GHz (ISM band)	2.4 GHz(ISM band)
	Frequency hopping spread spectrum	Frequency hopping spread spectrum
1 Mb/s	10 Mb/s	11 Mb/s (up to 54 Mb/s in 5 Ghz)
Security Bug		
Most expensive	Medium	Least expensive

Table 1. Wireless Network Criterion

The wireless SDDCPDD device will operate like the transmitter/receiver device in the picture below.

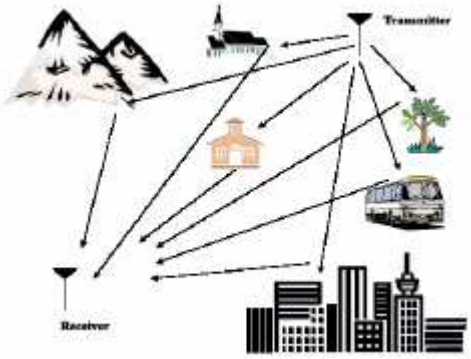

Figure 4. Similar Simulated SDDCPDD Transmission

What makes the 802.11x (IEEE Standard) Wireless Device such an attractive device for this application is its ability to apply a method of security in the system. Security means to encrypt and secure disseminated (propagated) packets. Once the packet is encrypted, it can be sent to its host and then checked for verification to be decrypted, and then routed to its appropriate protocol. There are always vulnerabilities to information, and not one bit or byte of information is free from hackers. However, we can make their job labor intensive and exhausting in trying to retrieve the information. One method of not allowing hackers to retrieve your information is to make it difficult for them to get access to the authentication keys (known as

authentication spoofing.) If the hacker gets hold of your plaintext along with two cipher-text packets, then the security of the information is violated and the key that goes along with the packets have been discovered, and more than likely he/she or they have infiltrated your system and have access to all your pertinent information.

Authentication is another method that can be used to prevent hackers from retrieving your information. Another method is to have the data encapsulated and check-summed to see if the host verifies that the message that has been sent and encapsulated is all intact. Using PostgresSQL and JDBC lower the cost and risk of hackers getting hold of your information. This method is cheaper than using an encryption/decryption scheme. However, this method would not be the method of choice for military applications due to the high nature and security risks associated with military missions and military protocols. Hackers or even the enemy getting hold of information could sabotage an operation or mission, which leads to defining which interfaces (COTS/OTS) to use to mate the system.

5. SOFTWARE/HARDWARE COMPONENTS AND INTERFACES

Commercial Off the Self (COTS) items and Off the Shelf Software (OTS) used for the enhancement and conformance of the design should lower the cost, increase the return on investment, and accessorize the system-development design. COTS and OTS could provide a more innovative, cost-saving solution as opposed to trying to develop the SDDCPDD device/design from scratch. The problem with using COTS/OTS is that you may encounter unexpected hazards, failures, and injuries to those wearing the device. The result of not integrating the COTS/OTS into the current system can be devastating. COTS may not necessarily have to offer environmental and safety-related documentation to assess the potential hazards or factors contributing to potential risks. This would enhance the opportunity to examine the interactions being used (source code, system diagnostics checks, serialized data transmission and retrieval), and monitor how all interactions in the design process actually operate once the communication enhancements are configured.

6. RISKS ASSOCIATED WITH OTS/COTS

There are going to be some risks with the interoperability using OTS/COTS.

Risk	Mitigation Strategy
OTS/COTS	Conduct lots of testing between systems, subsystems, and communication devices to ensure and mitigate interoperability between all models
Timing Delay	Modeling and Simulation should help in problems that may occur with module testing.
Costs	N/A
New Technology	Conduct human-based testing (Soldier).
Testing	Concurrent Modeling and Simulation throughout the Process.
Real-Time Processing of Information	Conduct testing, isolation of critical and non-critical events, and add a faster processor.

Table 2. Risk/Risk Mitigation Scheme

The Military Device and therefore SDDCPDD will have a designed base level secure software kernel within its design mechanism.[ii] The secure software kernel within Pacemaker/Defibrillator design detects significant failures of the hardware by a built-in-test or self-check control scheme to determine whether or not the device is properly operating and that the incoming/outgoing signals are sensed and whether the encoder/decoder, and processor is properly functioning. This feature was added as a way of detecting critical parameters in the presence of environmental or stresses that may degrade performance like that of chemical electrolyte within the body. Electrolyte from the body will not cause a problem or be considered a risk associated with the OTS/COTS for military applications. Timed system sequence latencies, and communication anomalies will also have to be monitored to handle the digital communication schema.[iii]

7. DIGITAL COMMUNICATION

Digital communication offers several advantages over analog signals. It offers increased immunity to channel noise and external interference. It offers flexibility of system operation. It provides a common format for the transmission of different kinds of message signals, whether they are voice, video signals,

or computer data. It also can be used to provide improved security of communications through the use of encryption technology. The other advantage to using digital communication is that it provides a method for allowing the "integration of diverse sources of information into a common format." [iv]
Since the signal has to ride on a wave of communication, normally an acoustic wave, or light wave; the signal (input/output information) has to be converted back and forth from analog to digital. Digital communication within the Military Device would have to have a feedback control for data recognition and verification. One of the disadvantages of digital communication as compared to acoustic wave is the problem of fading. Using frequency agility/hopping can solve the problem with fading by selecting one band of frequencies that is strong enough and agile enough to be transmitted across a medium without being interrupted. These frequencies are radiated by an antenna, similar to radar on how it emits pulses of electromagnetic energy to a distant object. The antenna is very important for transmitting and receiving information.

The formula for which a signal is sent out via digital communication is

as follows:

P_r = the power available at the receiver input (dBm)

P_t = Transmitter power output (dBm)

L_p = Free space losses (dBm)

G_t = Transmitter antenna gain (dB)

G_r = Receiver antenna gain (dB)

L_t = Transmission line losses transmit side (dB)

L_r = Transmission line losses receiver side (dB)

$$P_r = P_t - L_p + G_t + G_r - L_t - L_r$$

There are losses associated with signals being sent via cables or wireless application. These losses can be calculated to determine the maximum loss and strength of the signal being sent.

The Lp, which is the free space losses, is given by the formula:

$$L_p = 32.4 + 20 \log (f) + 20 \log (d)$$

f = frequency d = distance.

When sending wireless information the antenna chosen has to produce a maximum array factor (AF). The maximum array factor causes the signal from the antenna from within the device to be able to transmit enough impedance to reach the receiver while still maintaining a low-level power transfer. A low-level power transfer would allow the signal to be sent to its destination without causing any cell damage or harmful effects to the body. The low-level power transfer is chosen for the SDDCPDD because it offers minimal harmful effects of radiation according the 2 W/kg averaged over 10g of tissue put out by the safety transmission regulation and the FDA. The power delivered to the receiver is known by:

P_r = Powered delivered to the receiver

I = current

R = resistance

V = voltage

R_{in} = Input resistor in the system

Z_L = Load resistor

R_L = (2 R_{in} for max power output)

$$P_{max} = V^2_{incicent}/4R_{in}$$

Therefore, if V_{oc} (open-circuit voltage) is induced into the antenna terminals, then $Z_{in} = R_{rad} + jX_{in}$ (This is the antenna's impedance), and the impedance to the transmission line feeding the antenna. A_e (Effective area of a receiving antenna as the ratio of the time-average power received) is a measure of the ability of the antenna to extract energy from a passing EM wave. Therefore for maximum power transfer output (signal from the antenna) like that of the circuit shown for Rin and RL, the maximum power transfer is $V_{oc}^2/8\ R_{rad}$

$$P_r = \tfrac{1}{2}\ V^2_{incicent}/4R_{in}(R_{in})$$

This power is known as the incident power wave front effective area, or effective aperture. The physical area also known as the aperture area (surface area of the antenna) can be defined as

$$A_e = G\ (\lambda/4\pi)$$

To calculate the minimum transmitted power needed to send a signal from a device to its destination you would have to know the distance between the transmitting and receiving station, and the directed gain of the transmitter and receiver.

G_t = Transmission gain

G_r = Receiver gain

P_r = Power received

Given: Distance (d) = 100 λ

Transmitter gain = 12.5 dB

Receiver gain = 9 dB

Power received = 2.5 mW

With all of these factors being given, the scenario is as follows:

For a distance of 100 λ from the transmitting station to the receiving station, and a transmitting device gain of 12.5 dB and a receiving station gain of 9 dB, and if the power to be received is 2.5 mW, what is the transmitted power for signal transmitting from the device? To figure out the transmitted power, you would have to rearrange the formula and go through the following method of calculations.

$$G_t\,(dB) = 12.5\ (dB) = 10 \log^{10} G_{t,}$$

$$G_t = 10^{1.25} = 17.78$$

$$G_r = 10^{0.9} = 7.94$$

$$P_r = G_t\, G_r\, (\lambda/4\pi r)^2\, P_t$$

P_t transposed

$$P_t = 2.5mW\ (\ 4\pi\ X\ 100\ \lambda/\lambda)^2\ *\ (1/\ G_t\, G_r)$$

Thus,

$$P_t = 27.9\ W$$

The calculated transmitted power coming from the device is much higher than the requirement set by the FDA, therefore the SDDCPDD or Military Device would have to be adjusted. The adjusted transmitted power would have to be done automatically to be an effective part of the design scheme. The adjustment of the gain and signal strength power to achieve maximum safe output less than 2 W/10 g still has to be achieved. If you increase the gain from 12.5 to 25 dB, you would notice that the power transmitted P_t from the SDDCPDD thus Military Device is 1.25 mW, which is much lower than the maximum allowable power that can be transmitted from the device, and yielding good results. If you notice from the last calculation, there was too much power being transmitted from the device, and this would have caused a violation of the mandate put out by the FDA, and the FCC. Putting boundary conditions within the SDDCPDD to adjust the power output levels would give the device the opportunity to function optimally and still produce good results. However, if there is a need or emergency, the device may be required to send the maximum power output to the receiver. Controls will be conducted at all cost to ensure all measures are considered before this condition is warranted. The calculations in the first analysis yielded a power level of almost 15 times what is required by the signal safety transmission regulation commission and the FDA, and violate the power requirement.

Distance (d) = 200 λ

Transmitting Gain = 25 dB

Receiver Gain = 18 dB

Power Received = 5 mW

With all of these factors being given, the scenario is as follows:

If a gain of 25 dB and 18 dB is used for transmitting and receiving a signal between a distance of 200 λ from the transmitting and receiving antenna, and the power to be received is 5 mW, then the minimum transmitted power from the transmitter would be as follows:

$$G_t\,(dB) = 25\ (dB) = 10 \log^{10} G_{t,}$$

$$G_t = 10^{2.5} = 316.2$$

$$G_r = 10^{1.8} = 63.1$$

$$P_r = G_t\, G_r\, (\lambda/4\pi r)^2\, P_t$$

P_t transposed

$$P_t = 5mW\ (\ 4\pi\ X\ 200\ \lambda/\lambda)^2\ *\ (1/\ G_t\, G_r)$$

Thus,

$$P_t = 1.583\ W$$

This is more reasonable or safe for the amount of power you would want to come out of an antenna from an individual.

8. SYSTEM SAFETY

Antennas chosen for wireless communication requires the antenna to be of proper dimension to produce a maximum array factor (AF). The maximum array factor causes the signal from the antenna to be able to transmit enough impedance to reach the receiver while still maintaining a low-level power transfer. A low-level power transfer would allow the signal to be sent to its destination without causing any cell damage or harmful effects to the body. The FCC's exposure guidelines specify limits for human exposure to RF emissions from hand-held mobile phones in terms of Specific Absorption Rate (SAR). SAR is a measure of the rate of absorption of RF energy by the body. The allowable or safe limit for persons using a mobile phone is a SAR of 1.6 watts per kg (1.6 W/kg), and is considered as being the average power of Watts over one gram of tissue. Compliance with this limit must be demonstrated before the FCC approves or grant the use of cellular telephones for marketing of a

phone in the United States. Somewhat less restrictive limits, e.g., 2 W/kg averaged over 10 grams of tissue, are specified by the ICNIRP (International Commission on Non-Ionizing Radiation Committee) guidelines used in Europe and some other countries. The low-level power transfer is chosen for the SDDCPDD/Military Device because it offers minimal harmful effects of radiation according the 2 W/kg averaged over 10g of tissue put out by the safety transmission regulation and the FDA.

The unique feature of the heart is that each individual has a certain heart rhythm that is uniquely identified. Each individual device can be setup for a specific user, so no one else may attempt to fool the system by using a device not set-up for them. Since the device is tagged for the specific user it was issued to, the stats of the new person would read differently from the intended user. This would register a fault that would be sent to alert command and control or medical that there has been a change is this individual's hearth rhythm. This would give command and control an indication that something has gone wrong with that individual. They could then investigate what has happened to that individual, thus finding out who has taken possession of the device.

9. SDDCPDD DESIGN CONCEPT USED FOR MILITARY APPLICATIONS

The SDDCPDD/Military Device is self-diagnostic, individual specific, and serialized, therefore allowing stored information within the device to be sent via wireless communication to a database, data warehouse/data store to be used for future reference, statistics, and history. Other advantages are that the device allows for digital control, wireless communication, database verification, system safety, and security. The SDDCPDD or Military Device would have to be designed and tested based on military specifications with military communication requirements, thus as military communication signals have undisclosed frequencies that are different from those used by civilian medical devices. Low frequency is always best to use since everyone is using higher frequencies these days. The problem associated with low frequencies is the power associated with its losses. However, boosters will give the device the extra power levels it needs to process the signal to the receiving point. The signal could also be coupled to provide a higher gain.

The military has explored similar devices, such as the Warfighter Physiological Status Monitor (WPSM). The WPSM tackles concepts based on the body stresses (fatigue, mental, heat exhaustion, or respiratory failure) which is quite different from the SDDCPDD/Military Device. This paper addresses a need, finalized for a formulate solution.

REFERENCES

[i] Canadian Medical Hall of Fame [http://www.ewh.ieee.org/reg/7/diglib/library/electricity/pdf/P_one_3.pdf], February 2002.

[ii] Nancy G. Leeveson. Safeware. *System Safety and computers*, 1:410 September 1995.

[iii] Nancy G. Leeveson. Safeware. *System Safety and computers*, 1:418 September 1995.

[iv] S. Haykin, An Introduction to Analog and Digital Communications, Wiley, New York, pp 177-178, 1989.